PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-224606
(43)Date of publication of application : 08.08.2003

(51)Int.CI. H04L 12/58
G06F 13/00
H04L 9/08

(21)Application number : 2002-059516
(22)Date of filing : 28.01.2002

(71)Applicant : SUZUKI TOMOMASA
(72)Inventor : SUZUKI TOMOMASA

(54) TECHNIQUE FOR PROTECTING PERSONAL INFORMATION BY CIPHERING ELECTRONIC MAIL ADDRESS WHEN SENDING AND RECEIVING ELECTRONIC MAIL TO AND FROM ARBITRARY PARTY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide environment wherein when electronic mail addresses of individuals should be secret like a communication site in the Internet environment, a document can be sent to a transmission destination without requiring mutual electronic mail addresses which are sent and received.
SOLUTION: (a) An electronic mail server has electronic mail addresses registered by unspecified accessing persons and issues serial numbers. (b) A cipher is generated from two serial numbers and a ciphered electronic mail address to the electronic mail server is generated on the basis of it. (c) The electronic mail server having received an electronic mail calculates the transmission destination address as the ciphered electronic mail address back to a cipher to calculate two serial numbers. (d) The electronic mail server acquires two electronic mail addresses from the two serial numbers and transmits the body of the received electronic mail to the two electronic mail addresses. (e) The electronic mail server erases the transmission source address of the electronic mail to be sent.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－224606
（P2003－224606A）
(43)公開日　平成15年８月８日(2003.8.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	12/58	１００	Ｈ０４Ｌ　12/58	１００Ｚ	５Ｊ１０４
Ｇ０６Ｆ	13/00	６０１	Ｇ０６Ｆ　13/00	６０１Ａ	５Ｋ０３０
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ　9/00	６０１Ｃ	

審査請求　未請求　請求項の数１　書面　（全 3 頁）

(21)出願番号　特願2002－59516(P2002－59516)

(22)出願日　平成14年１月28日(2002.1.28)

(71)出願人　500366473
鈴木　伴優
愛知県一宮市天王１丁目４番31号
(72)発明者　鈴木　伴優
愛知県一宮市天王一丁目四番三十一号

Ｆターム(参考)　5J104 PA08
5K030 GA15 HA06 LD19

(54)【発明の名称】　任意の相手と電子メールを送受信する際、電子メールアドレスを暗号化し、個人情報を保護する技術

(57)【要約】　（修正有）
【課題】インターネット環境下における交流サイトのように各個人の電子メールアドレスを秘密にしなければならない場合、送受信するお互いの電子メールアドレスを必要としない状態で送信相手に文書を送信できる環境を提供する。
【解決手段】（イ）　電子メールサーバは不特定のアクセス者により電子メールアドレスを登録され、通し番号を発行する。（ロ）　２つの通し番号より暗号を作成し、それを元に電子メールサーバへの暗号電子メールアドレスを作成する。（ハ）　電子メールを受信した電子メールサーバは暗号電子メールアドレスである送信先アドレスを下に暗号を逆算し、２つの通し番号を算出する。（ニ）　電子メールサーバは２つの通し番号より２つの電子メールアドレスを取得し、受信した電子メールの本文を２つの電子メールアドレスに電子メールを送信する。（ホ）　電子メールサーバは送信する電子メールの送信元アドレスを消去する。

【特許請求の範囲】
【請求項１】（イ）　電子メールサーバー（０１）は不特定のアクセス者により電子メールアドレス（０２）を登録され、通し番号（０３）を発行する。
（ロ）　２つの通し番号（０３）より暗号（０４）を作成し、それを元に電子メールサーバー（０１）への暗号電子メールアドレス（０５）を作成する。
（ハ）　電子メールを受信した電子メールサーバー（０１）は電子メールの送信先アドレス（これは暗号電子メールアドレス（０５）である）を元に暗号（０４）を逆算し、２つの通し番号（０３）を算出する。
（ニ）　電子メールサーバー（０１）は２つの通し番号（０３）より２つの電子メールアドレス（０２）を取得し、受信した電子メールの本文を２つの電子メールアドレス（０２）に電子メールを送信する。
（ホ）　電子メールサーバー（０１）は送信する電子メールの送信元アドレスを消去する。
以上の如く構成された環境
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明はインターネット環境下で、不特定の個人（０６）同士がお互いの電子メールアドレス（０２）を秘密にしつつ電子メールを送受信する為の技術である。
【０００２】
【従来の技術】現在のものでの流れは、
１．個人（０６）が交流サイト（０７）にアクセスし、電子メールアドレス（０２）を含む秘密情報（０８）を個人情報（０９）として登録することで、通し番号（０３）を取得する。
２．交流サイト（０７）に通し番号（０３）でアクセスし、本人以外の登録された個人（０６）と交流する手続きを行う。
３．交流サイト（０７）に通し番号（０３）でアクセスし、交流する本人以外の登録された個人（０６）に対して文書を作成、送信作業を行う。
４．交流サイト（０７）に通し番号（０３）でアクセスし、文書を受け取った個人（０６）は、その文書を送信した個人（０６）に対して返信文書を作成し、その文書の送信作業を行う。
以上の様に、電子メールアドレス（０２）の様な秘密情報（０８）の流出を防ぐために通し番号（０３）を発行し、何をするにも交流サイト（０７）にアクセスする必要があり、簡単で且つ短時間で文書を交流相手に送信する事が困難である。
【０００３】
【発明が解決しようとする課題】インターネット環境下において文書を任意の個人に送信する場合は、送信相手の電子メールアドレス（０２）に対して電子メールを送信する事が一般的な方法であるが、交流サイト（０７）

の場合は、各個人（０６）の電子メールアドレス（０２）を秘密にしなければならないため、一般的な方法である電子メールを使用するものの送受信するお互いの電子メールアドレス（０２）を必要としない状態で送信相手に文書を送信できる事が理想である。本発明は、その欠点を取り除くために考案されたものである。
【０００４】
【課題を解決するための手段】以下の技術を交流サイト（０７）の電子メールサーバー（０１）に組み込む。
１．電子メールサーバー（０１）はアクセスのあった個人（０６）の電子メールアドレス（０２）を含む秘密情報（０８）を蓄積し、その個人（０６）に通し番号（０３）を発行する。
２．電子メールサーバー（０７）は通し番号（０３）を持つ個人（０６）が交流手続きを行った他の通し番号（０３）を持つ個人（０６）の通し番号（０３）を元に可逆的な計算を行う事で暗号（０４）を作成、それを元にした電子メールサーバー（０１）宛ての暗号電子メールアドレス（０５）を発行する。
３．電子メールサーバー（０１）は交流手続きをした通し番号（０３）を持つ２人の個人（０６）に対して、発行された暗号電子メールアドレス（０５）を通知する。
４．電子メールサーバー（０１）は暗号電子メールアドレス（０５）により受信した電子メールの送信先である暗号電子メールアドレス（０５）を元に逆計算を行う事で２人分の個人（０６）の通し番号（０３）を取得し２人分の個人（０６）の電子メールアドレス（０２）を含む秘密情報（０８）を取得する。
５．電子メールサーバー（０１）は受信した電子メールの文書を２人の秘密情報（０８）より取得したそれぞれの電子メールアドレス（０２）に対して送信する。また、その時に発信者情報を削除する。
以上の技術により、交流する各個人（０６）は各自の電子メールアドレス（０２）を知られる事なく最低限の作業で、文書を送受信する事ができる。
【０００５】
【発明の実施の形態】以下、本発明の実施例について説明する。
１．個人（０６）が交流サイト（０７）にアクセスし、電子メールアドレス（０２）を含む秘密情報（０８）を個人情報（０９）として登録することで、通し番号（０３）を取得する。
２．電子メールサーバー（０１）はアクセスのあった個人（０６）の電子メールアドレス（０２）を含む秘密情報（０８）を蓄積し、その個人（０６）に通し番号（０３）を発行する。
３．交流サイト（０７）に通し番号（０３）でアクセスし、本人以外の登録された個人（０６）と交流する手続きを行う。
４．電子メールサーバー（０７）は通し番号（０３）を

持つ個人（０６）が交流手続きを行った他の通し番号（０３）を持つ個人（０６）の通し番号（０３）を元に可逆的な計算を行う事で暗号（０４）を作成、それを元にした電子メールサーバー（０１）宛ての暗号電子メールアドレス（０５）を発行する。

５．電子メールサーバー（０１）は交流手続きをした通し番号（０３）を持つ２人の個人（０６）に対して、発行された暗号電子メールアドレス（０５）を通知する。

６．交流手続きをした通し番号（０３）を持つ２人の個人（０６）は交流サイト（０７）より暗号電子メールアドレス（０５）の通知を受信する。

７．個人（０６）は暗号電子メールアドレス（０５）を送信先として、交流相手への文書を作成し、電子メールとして送信する。

８．電子メールサーバー（０１）は暗号電子メールアドレス（０５）により受信した電子メールの送信先である暗号電子メールアドレス（０５）を元に逆計算を行う事で２人分の個人（０６）の通し番号（０３）を取得し２人分の個人（０６）の電子メールアドレス（０２）を含む秘密情報（０８）を取得する。

９．電子メールサーバー（０１）は受信した電子メールの文書を２人の秘密情報（０８）より取得したそれぞれの電子メールアドレス（０２）に対して送信する。また、その時に発信者情報を削除する。

１０．文書を送信した個人（０６）と交流相手の個人（０６）は電子メールサーバー（０１）が送信した電子メールを受信する。

以上の工程により、各個人（０６）は交流相手となる個人（０６）の電子メールアドレス（０２）を知りうる事なく、交流することができる。

【０００７】

【発明の効果】１．交流サイト（０７）へのアクセスが最小限で済む。

２．手軽な電子メールの送受信で交流を済ます事ができるので、交流サイト（０７）へアクセスする手段が無い環境（電子メール送受信機能搭載電話等）でも交流が可能である。

３．交流相手の電子メールアドレス（０２）等の秘密情報（０８）に振れる事なく、電子メールの送受信が可能となる。

４．交流相手に文書が送信されたかどうかを、その文書が自分に送信されるのを確認する事で、同時に確認する事が可能となる。

５．暗号（０４）を使用する事により、交流手続きを行っていない通し番号（０３）を持つ個人（０６）が、その交流や秘密情報（０８）に侵入する事を不可能とする事が可能となる。